IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,

Plaintiffs,

vs.

CIVIL ACTION FILE
NO. 1:17-CV-2989-AT

BRAD RAFFENSPERGER, ET AL.,

Defendants.

REMOTE VIDEOTAPED ZOOM DEPOSITION OF
DAVID HAMILTON

January 18, 2022
10:06 A.M.

Lee Ann Barnes, CCR-1852B, RPR, CRR, CRC

INDEX TO EXHIBITS

INDEX TO EXHIBITS

INDEX TO EXHIBITS

(Original exhibits are attached to the original transcript.)

VIDEOGRAPHER: Would the court reporter please swear in the witness.

DAVID HAMILTON, having been first duly sworn, was examined and testified as follows:

EXAMINATION

BY MS. KAISER:

Q. Good morning, Mr. Hamilton.

A. Good morning.

Q. Can you please state your name and address for the record?

A. David Hamilton, 4570 Summerwood Drive, and that's in Cumming, Georgia 30041.

Q. Thank you.

Are you represented by counsel today, sir?

A. For the purposes of this proceeding, yes, by Carey Miller.

Q. Okay. All right. Have you ever been deposed before?

A. Not via video, no.

Q. All right. Let me just walk you through a couple of rules of the road, just to -- just to level-set here.

So I'm going to be asking you a series of questions. I'll try to make my questions clear, but if you do not hear a question or you don't

A. Sorry.

Q. I think time is a little confused for all of us because of COVID.

A. The years, yeah.

Q. Right. All right. So thank you.

So when did you first learn that we wanted to take your deposition in this case?

A. I guess middle of last week.

Q. Okay. And how did you learn that?

A. I -- we got the -- I got an email from -- I'm blanking on it -- Ryan Germany and -- and said that I may get a subpoena. And lo and behold, I did. So...

Q. So Mr. Germany reached out to you first about this deposition; is that right?

A. Just to let -- let me know that it may be coming.

Q. Did you meet with -- with counsel for the State before today in preparation for the deposition?

A. Yes, ma'am.

MR. MILLER: Objection on relevance.

BY MS. KAISER:

Q. And when did you do that?

A. I guess last week. I can't remember the

A. Okay. I'm sorry. I probably talked over the end of your question. I'm sorry.

Q. No problem. Thank you.

Have you spoken with anyone besides counsel for the State about this deposition?

A. No. I take that back. Yes, my wife.

Q. What did you tell your wife with respect to the deposition?

A. Just that I was being deposed for the case that I gave testimony in a couple years ago. So...

Q. Okay. Thank you.

And I believe you said that the way that you learned about the deposition was receiving an email from Mr. Germany; is that correct?

A. Yes, ma'am.

Q. And then -- so that was -- was that on a personal email address?

A. Same one that you have here, yeah.

Q. I'm -- okay. Yeah.

Did anybody from the State's -- from the Secretary of State's office or their counsel contact you last year regarding having your deposition taken in this case?

A. No.

MR. MILLER: Objection. Relevance.

BY MS. KAISER:

Q. Do you have any idea why the Secretary of State's counsel told us that they were unable to locate you in late 2021?

A. I --

MR. MILLER: Objection. Relevance. Lack of foundation.

BY MS. KAISER:

Q. You may answer the question, Mr. Hamilton.

A. No, I don't.

Q. Do you live at the same home address as when you worked at the Secretary of State's office?

A. Yes, ma'am.

Q. And did the Secretary of State's office have that address on record, to your knowledge?

A. Probably not, because I wasn't an employee.

Q. Understood.

But they did have your email address; is that correct?

A. Yes, ma'am.

Q. And so they were able to contact you when they tried?

A. I believe so, yes.

Q. Thank you.

an email from dhamilton@imperialhealth.com dated July 10, 2020.

Do you see that?

A. I do.

Q. And is that your -- is that your email address?

A. It was at Imperial Health down in Louisiana, right. This was a fractional --

Q. And --

A. -- engagement between the two and I was half-timing it, sometimes in Louisiana, sometimes at the State.

Q. Understood.

So during the time you were working with the Secretary of State's office, you were also working with Imperial Health; is that right?

A. Correct. And other clients as well.

Q. Okay. If you look -- if you look through this email chain -- and it starts at the -- it begins at the end, if you will, so the first email is at the bottom.

A. Okay.

Q. And this looks to be -- the subject of this email chain is "FortaliceSOSGA - Rules of Engagement."

Do you see that?

A. Uh-huh.

Q. All right. And there's an email from Paul Brandau at Fortalice Solutions.

Do you see that?

A. Right.

Q. All right. What is Fortalice Solutions?

A. Fortalice is a -- is a vendor, a partner, of the State that provides security services, pen testing, pay-as-you-go kind of investigative services on things that are security based.

Q. Okay. And Mr. Brandau sent this email to Merritt Beaver, as well as you and some others in the Secretary of State's -- or, sorry, and some others at Fortalice; is that right?

A. Correct.

Q. And who is Mr. Beaver?

A. I'm sorry?

Q. Who is Merritt Beaver?

A. He's the CIO for the State of Georgia -- for the Secretary of State of Georgia.

Q. Okay. And then on the first -- first page of the document, you see a response from Mr. Beaver to you and Mr. Brandau.

Do you see that?

A. Yeah, I do.

Q. Okay. And so does it appear to you that this document relates to your work for the Secretary of State's office?

A. It does.

Q. Okay. And your response at the top of the page, where we started, that was sent from your Imperial Health email address; is that correct?

A. Right. Just on error --

Q. Did you --

A. -- because -- because -- because I was probably down there and I didn't change the thing at the top of Outlook.

Q. Did you ever collect any emails from your Imperial Health email account for the purposes of this case?

A. No, ma'am.

Q. Okay. You can put that document aside for now.

A. Okay.

Q. I'm just going to ask you a few questions about your background, Mr. Hamilton.

Where did you get your undergraduate degree?

A. I did not go to college.

Q. Oh, okay. Do you have any certifications or -- or professional -- I believe you have some professional certifications; is that correct?

A. I do, yes, ma'am.

Q. Can you tell me about those?

A. I have a CISSP, which is the certification for information security professionals. I have a CISM through ISACA. I have a CDPSE, which is a privacy standard certification. I have a healthcare-specific privacy and compliance certificate and also a certified C|CISO certificate.

Q. That's C-S-E-L?

A. C, and then a bar, C-I-S-O. Right.

Q. Would you say that you have any training in cybersecurity?

A. Yes, ma'am.

Q. How long have you worked in the cybersecurity field?

A. Probably about 15 years now.

MS. KAISER: Pull up Tab 1, please.

BY MS. KAISER:

Q. I'm going to add Exhibit 2 to the Exhibit Share.

A. Okay.

(Plaintiffs' Exhibit 2 was marked for

identification.)

THE WITNESS: Oops, it logged me out. Hang on a second.

BY MS. KAISER:

Q. Sure.

A. Crap. I'm looking at the wheel. Hang on. It's thinking.

Okay. Number 2.

Q. Do you recognize this document, Mr. Hamilton?

A. Uh-huh. Yes.

Q. Is this a copy of your profile from LinkedIn?

A. Looks like it.

Q. And is this something that you update regularly?

A. I haven't in a while. Since -- since I landed at -- at Shepherd, there's not much point in it.

Q. Okay. And that was -- when did you begin with Shepherd?

A. June, right as I left TrustPoint.

Q. In 2021?

A. Yes, ma'am.

Q. On -- at the bottom of page 1 of this

document, it indicates that you worked for TrustPoint Solutions from October 2013 to June 2021; is that correct?

A. It is.

Q. And what is TrustPoint Solutions?

A. They're a provider of security and infrastructure services predominantly in healthcare. They have some business outside in the public sector.

Q. Sorry. I think you mentioned this, but during the time that you had the title of chief information security officer for the Georgia Secretary of State's office, were you employed by TrustPoint Solutions?

A. Yes, ma'am.

Q. So did you do work for the Secretary of State's office on a contract basis?

A. No, not directly. Always through TrustPoint.

Q. So you mean you, yourself, were not under contract; the company --

A. Correct.

Q. -- TrustPoint was?

A. Correct.

Q. How much time did you spend per month on

work at the Secretary of State's office, roughly?

A. I guess it averaged out to be probably half-time. There was some spikes there where it was more full time as things ramped up for events such as elections and things, incorporations. End of year was a pretty busy time for the corporation side. But as you look across, I would imagine it would compute to be about half-time.

There were some times where I didn't -- wasn't there at all during a week because I was at a different client.

Q. When you say "there at all," were you physically at the Secretary of State's office?

A. Yes, ma'am.

Q. And when did you begin working for the Georgia Secretary of State's office?

A. Summer of 2018. That's when the engagement first began.

Q. And so from roughly summer of 2018 until June of 2021, you spent approximately half your time working on security issues for the Georgia Secretary of State's office; is that correct?

A. Yes, ma'am.

Q. And what were your responsibilities for the Georgia Secretary of State's office?

A. Just overseeing the -- the corporate information security program, which included the -- the election side as far -- insofar as it -- the registration side of the house. Not the Dominion side, but the -- the corporation side of the house, which is where you get a business license in Georgia, and then also the Bureau of Licensing, which is all the professional boards, the nursing board and the barbershop folks and all those folks. It's where you kind of go for -- that was the only place that had PHI, so -- protected health information.

Q. Understood. Okay.

And when you said -- you said that that encompassed the election side insofar as the registration side of the house.

Can you explain what you mean by that?

A. Well, there's -- there was a couple of different buckets, right? The -- the -- the main things that I was concerned with is the -- is the voter registration, the MVP site; security of the -- more or less the public-facing sites that managed the registration of a voter.

Didn't have anything to do with the tabulation of votes or the voting machines

themselves. All that was handled by the vendor.

Q. Interesting. Okay.

Who did you report to at the Secretary of State's office?

A. Mr. Beaver. Merritt Beaver, the CIO.

Q. And did anybody report to you?

A. Yes. There was -- we had a couple of -- three. At one point there was one, then it got back up to three when we restaffed. There were several names in there. Do you want me to try to recall them?

Q. Yes, if you can.

A. Okay. When I got there, it was -- I just can't recall his name. Heavyset fella. I can't -- probably have to go to LinkedIn to figure that one out. I can't recall his name.

When I left --

Q. Do you recall -- I'm sorry. Please finish.

A. I was just going to say when I left, I can tell you who those folks were.

Ronnell Spearman, who is -- who I think is still there; Kevin Fitts; and then there was one person that hired just as I was leaving. I actually never got to meet him in person and I can't recall

his name.

Q. Do you recall the titles of the -- the people that reported to you?

A. Yeah. Just security analyst.

Q. As part of your work with the Secretary of State's office, did you work with any outside vendors?

A. Yes, ma'am.

Q. What vendors were those?

A. Probably the largest being Fortalice. They were kind of my right hand, made up for us not having a big staff of folks.

Beyond that, we had Dell Secureworks. We had Palo Alto. A lot of the providers of the solutions that we used. Critical Start would be an example. Just -- Clawless [phonetic].

Q. And I think you -- you may have mentioned this before, but what services did Fortalice provide for the Secretary of State's office?

A. Security services. They did pen testing. You know, we have an annual pen test where we have somebody come in from the outside.

And also incident response. So if there was something that came up where we needed some investigative specialty, kind of a subject matter

expert on intrusion or one of those guys, they have a bench of people.

They're -- they hired on about the same time that TrustPoint did. We kind of came in about the same time. And we decided to use Fortalice for that half and -- and TrustPoint for the guy that sat in the seat, which was me.

It actually started off being Gaylon Stockman, but once things got ramped up, Gaylon left TrustPoint for another job, so it ended up being just me. The idea was to kind of alternate us back and forth to give enough time, but it just didn't work out that way in the end.

Q. So originally the job was supposed to be split between two people from TrustPoint --

A. Correct.

Q. -- TrustPoint?

A. Yeah, that was how -- that was how the SOW was written, statement of work.

Q. And would that have provided more hours overall of support from TrustPoint, more like a full-time person?

A. No, I think the statement of work was still half-time at that point, but the issue was that both Gaylon and I had other commitments that I

Q. As chief information security officer, would you say that you had a relatively senior position in the Secretary of State's office?

A. Yeah, as far as a contractor can go. You know, I didn't have any signing authority. I didn't have a budget. I didn't -- you know, it's not like a regular engagement where, you know, there's some distance there.

If -- if I was a full-time employee, it would have been a different situation, I think. But I relied on -- on Merritt for a lot of the back office-type operations, and most -- most of my engagement was -- there was basically making recommendations and just -- you know, "I think we should do this," and, you know, Merritt could say yea or nay and we went from there.

Q. Do you have a view on whether having a half-time chief information security officer was adequate for an entity the size of the Georgia Secretary of State's office?

MR. MILLER: Objection. Lack of foundation. Calls for speculation.

THE WITNESS: I can say that I do -- or I did, rather, in the past fractional CISO work for a lot of firms and it worked very well.

A. I -- I didn't spend an awful lot of time reading them. We just kind of glazed over them.

But, no, I -- I felt pretty good about my memory about things, what happened. So...

Q. Did you ever recommend to the Secretary of State at any point that they should have a full-time chief information security officer?

A. Yes.

Q. Do you recall approximately when you made that recommendation?

A. I think, basically, when -- when James Oliver -- he was my predecessor. He was a full-time employee.

I think initially when we came in, you know, our edict was to kind of coach him up and get him, you know, kind of more out there.

And James, very nice man, but he was kind of reserved and quiet, and it's kind of hard to do this job when you seal yourself in your office. You kind of have to be out there and evangelize security and get people excited about it, and he just didn't have that gene.

So I -- you know, when the Secretary of State made the decision to part ways with James, I really thought the next step was for me to help the

Secretary of State find another full-time employee.

In the end, it wasn't. What they decided to do is do a fractional kind of a situation where they'd continue that relationship and kind of let me sit in the chair.

That's not unheard of, but it's -- I mean, I would have rather have them have a full-time employee just for consistency, right? Because you never know if I'm going to get pulled away on another -- on another deal or -- you know. It would have been better, I think, to have a full-time, and I could advise that person kind of as a -- think of it as like a mentor relationship.

Q. And I believe you said that you didn't -- you personally didn't have a budget.

Did you ever make a recommendation that the chief information security officer should have a budget?

A. No. I mean, they -- they had a budget for security; it's just I wasn't -- I didn't have any signing authority. I couldn't go spend money. You know, I didn't have an expense account or anything like that.

Anything I wanted to spend money on, I had to go to -- go to Merritt for, and he worked it out

BY MS. KAISER:

Q. Did you have any --

A. -- the wrong place to put it.

Q. Did you have any involvement with making that transition of the Kennesaw server?

A. No, ma'am. No, ma'am. That was way prior. 2016, I guess. So...

Q. We've mentioned Fortalice several times now.

Are you aware that Fortalice conducted a series of cyber risk assessments for the Secretary of State's office in 2017 and 2018?

A. Yes, I -- I have knowledge of those.

Q. What role, if any, did you have in working with Fortalice on those cyber risk assessments?

A. The second one in 2018, I believe that was during my tenure, at least I got the report. The 2017, I think they just passed it to me as history. So...

Q. And can you tell me, in general terms, what Fortalice found in its 2017 and 2018 cyber risk assessments for the Secretary of State's office?

A. There was a number of items. They classified them as high, medium, low, based on their experience, and then gave us an opportunity to

either accept or -- or deny, you know, what was going on.

It gives us a good basis for kind of reprioritizing our work within the State to figure out where we should spend our money and time trying to go after the things that are the most vulnerable. It's a judgment call.

MS. KAISER: Can you pull up Tab 3, please.

(Plaintiffs' Exhibit 4 was marked for identification.)

THE WITNESS: Is there another document? I'm sorry.

BY MS. KAISER:

Q. It's being loaded right now.

A. Okay. I'm sorry.

Q. It takes a minute with larger documents, so apologies --

A. Gotcha.

Q. -- for the delay.

A. Okay. Exhibit B. Okay.

Q. So if you scroll down to the next page, you'll see this is the cover page of the report.

Do you recognize this as the 20- -- November 2018 report that Fortalice provided to the

Secretary of State's office?

A. I think so. Let me go down to the meat of it here. Hang on.

MR. MILLER: Mary, this is another sealed document. I can't recall from the 2019 hearing if we -- how we designated this.

THE WITNESS: Yeah, this kind of thing should never be made public, but I get it.

MR. MILLER: So, Mary, I'll -- I'll ask at this point if we treat it as attorneys' eyes only.

And, Ms. Marks, if you could please drop off for the period of time.

MS. MARKS: Sure, I will. And if you will let me know when I can safely come back on. Thank you.

(Ms. Marks left the Zoom deposition.)

BY MS. KAISER:

Q. Mr. Hamilton, have you had a chance to take a look at the document now?

A. I have, yep.

Q. And do you recognize this as Fortalice's 2018 Red Team Penetration Test and Cyber Risk Assessment?

A. I do, yep.

Q. If you could turn to page 8 of the report.
A. Okay.
Q. The top section there says "2017 Top Ten Risks Status in 2018."
Do you see that?
A. Correct.
Q. That next paragraph reads, "The following table lists the top ten risks from the Georgia Secretary of State's 2017 cyber risk assessment and progress made to date on those risks."
A. Right.
Q. If you skip one sentence, it says, "Of the top ten risks from the 2017 report, three were not tested during the 2018 assessment, three were remediated in the past year with compensating controls and three remain unresolved."
Do you see that?
A. I do.
Q. So do you understand this section of the report to address progress made on the top ten risks identified by Fortalice in 2017?
A. Uh-huh. Yes.
Q. Do you know why three of those top ten risks were not tested in 2018?
A. I do not. Usually, it's a -- when a --

when a security firm does a -- a pen test or a security assessment, they use last year and the current year to show progress or show kind of a trend, are you getting better or are you getting worse. So usually you test the same things.

The only reason I would think that we missed is if they were specifically taken out of scope.

Q. Okay. And this report says that of the top ten risks identified in 2017, only three had been remediated in 2018; is that correct?

A. That's what this states, correct.

Q. If you can flip to page 5 of the report.

A. Okay. Hang on. It's back. Hang on.

Okie-doke. I'm here.

Q. The second paragraph on page 5, it reads, "In order for Georgia Secretary of State to best protect the confidentiality, availability and integrity of data it holds in trust for the residents of Georgia, Fortalice recommends implementing the following controls."

Do you see that?

A. Right.

Q. And that first bullet point reads, "There are 20 recommendations...."

Do you see that?

A. I do.

Q. And are those recommendations detailed on pages 6 and 7 of the report --

A. I believe so.

Q. -- in this table?

A. Yeah.

Q. What steps did the Georgia Secretary of State's office take to implement these 20 recommendations from Fortalice?

A. I can't speak to the first half of that year because I wasn't there, but it might have had something to do with -- and this is a little bit of speculation on my part -- is that that might have been the reason for our involvement, is that Merritt didn't feel like things were moving along fast enough.

So he wanted -- that was one of the things that we were to come in and coach up for James Oliver is to kind of get him excited about this stuff and get moving on some of these things that were identified.

And I think this was the list that I gave the status on I guess about halfway through the tenure. That was one of the exhibits or the

statements that I made to the Court.

So I don't know what the status is now, of course, because I've been gone six months, but they were well on their way to taking care of those and -- and others that were found along the way. So...

Security is -- itself truly is a -- it's a journey; it's not a destination. You're never done. I mean, there's always -- the threat landscape changes every day. Things change every day.

So, you know, it's a snapshot in time. At the time that Fortalice did this, this is what they found. They could have waited three weeks and did another one and found something else and not found three others. So it's just a snapshot in time.

Q. Sure.

At the bottom of page 5 of the report, the last paragraph there, it says, "Although Fortalice only explicitly recommends additional staff for one of the twenty findings, we believe that additional resources could accelerate the timeline for addressing the security risks in this report."

Do you see that?

A. I do.

Q. To your knowledge, did the Secretary of

MS. KAISER: Will you add Tab 4, please, Zach.

BY MS. KAISER:

Q. We're going to bring up the next exhibit, Mr. Hamilton.

A. Okay.

(Plaintiffs' Exhibit 5 was marked for identification.)

BY MS. KAISER:

Q. If you scroll down to the second page, I believe you -- you stated that you -- you know, you made a statement in this case.

Do you recognize this to be the declaration that you provided in this case?

A. Yes, ma'am. One of two, correct.

Q. Correct.

Let's see. This one is dated August -- August 25, 2020.

Do you see that?

A. That sounds about right, yep.

Q. Okay. Did you draft this document, sir?

A. I did.

Q. And the purpose of your declaration, as you mentioned, was to go through the recommendations from Fortalice and give a status update on how they

were being resolved or remediated; is that right?
A. Correct.
Q. I just want to walk through a couple of these.
So Number 2, the "Two-Factor Authentication," do you see that?
A. Uh-huh.
Q. It says the "Status" was "Accepted and Partially Remediated."
A. Uh-huh.
Q. Do you see that?
All right. And Number 5 was "Non-Unique Local Admin Passwords."
Do you see that?
A. I do.
Q. The "Status" was "Accepted and Compensating Control Applied."
Do you see that?
A. Correct.
Q. What did you mean by "compensating control applied"?
A. The long-term solution would be to go to a PAM, which is a privileged account management solution, but that's a pretty heavy lift financially.

wouldn't move that fix back into the code line, so the very next time they did a revision, they would re-break the thing.

And that is kind of a, you know, 101 change control operation. Somebody wasn't watching the store. So...

And we tried to help grow them. You know, we gave them a lot of feedback, probably a lot more than they ever wanted.

And then they were purchased by another firm, and that gentleman -- they had a CISO there. He's the gentleman that actually attested to the fact that their minimum security met the minimum based on what I had sent them. I think he was hopeful that it would get that way, but I had my -- like I said, I had my doubts, so to speak.

Q. All right. Well, going back to your declaration, Mr. Hamilton, we can -- we can keep walking through them one by one, but by my count, there were 11 out of 20 recommendations that, according to your declaration, had not been fully remediated.

A. Right.

Q. Does that sound about right?

A. (Nodded head.)

Q. Okay. And that was the status as of August 2020; correct?

A. Correct, so basically three months into my tenure. That's about right, yeah.

Q. Three months into your tenure. Okay.

And -- but that was nearly two years after Fortalice issued their cyber risk assessment in November 2018; is that correct?

A. Correct.

MR. MILLER: Objection. Lack of foundation.

BY MS. KAISER:

Q. And so nearly two years after Fortalice issued that report, at least half of their recommendations had not been fully implemented; is that correct?

MR. MILLER: Objection. Asked and answered.

THE WITNESS: It sounds like it, yeah.

BY MS. KAISER:

Q. Based on your experience and training, does it seem reasonable to have a cybersecurity vendor identify security risks in your system and then not take recommended steps to address those risks for nearly two years?

MR. MILLER: Objection to form. Lack of foundation. Calls for speculation.

THE WITNESS: In -- in my professional opinion, it's not uncommon. Some of -- some of the things that we're faced with have budgetary constraints.

The bottom line is we present -- as security people, we present to the business and say, "Here's the nine things we've got to do. You know, what's our bucket of money look like? What does it take, you know, horsepower, people, whatever?" And then the business makes the decision finally on -- on what -- what to focus on. We make recommendations and then we move on those.

But we made pretty good headway, I think --

BY MS. KAISER:

Q. Were you pushing the Secretary of State's --

A. -- before I left. So...

Q. Were you pushing the Secretary of State's office to move faster or make more headway on these recommendations from Fortalice?

A. Yes, ma'am. I was kind of the evangelist,

and, yeah, I was -- I was not shy about it. So...

Q. Why were you pushing that?

A. Just to get -- get moving, right? We had the time and some of the things, like was outlined, are low cost or no cost. It doesn't mean that it -- I mean, no cost is nobody has to write a check to a vendor.

But the big thing is -- is the headcount. It's the talent that you have in-house that are able to do these tasks. And a lot of my time there was -- was training, mentoring, kind of teaching people how to kind of ramp things up. So -- yep.

Q. Have you -- you felt that these recommendations from Fortalice were good ones, correct, that would improve the security of the system?

A. Yeah. That's why on -- on the -- on the statement where I said "Accepted" -- in any -- in any situation where a -- a security firm comes in and does an assessment or a pen test and they present you with the findings, you're able to accept those or not accept them.

An example of not accepting is either it was out of scope or something that had long been fixed and they missed it. You know, things like

that.

So in most of these cases, I believe I accepted most of these because I verified that they were still valid.

Q. Has Fortalice done any additional work for the Secretary of State's office since the penetration testing in 2018?

A. I -- I -- they had an annual -- they had an annual test and assessment, a pen test.

Q. And when you say "pen test" --

A. I know we --

Q. -- is that --

A. Penetration test. That's somebody from the outside tries to get in. There's three forms of that. There's, you know, the white hat, the black hat, and the gray hat.

So this was very much -- we did not give them the keys to the castle. We wanted them to replicate the outside world, so that becomes a black hat operation.

Gray hat is when you give them a little bit of a path, you know a little bit about the environment.

And then white hat, of course, is you give them carte blanche to the environment and then they

just go -- usually that's an internal pen test. But all of these were external.

Q. And to your understanding, Fortalice did one of these pen test assessments each year since --

A. Yes, ma'am.

Q. -- 2018?

And did they test the -- the entire part of the Secretary of State's network or -- or portions of it in those years, do you know?

A. Most of it was just the business network, right? It was the business network and the public-facing websites, nothing specific to --

You know, every business has a certain number of IP addresses that face the public, and I think in previous years, because of cost, they had kind of truncated that list a little bit. Because they do charge per IP address.

And I know one of the years that I was there, I went ahead and had them test everything, every public IP address that we had. It was expensive to do, but you -- you kind of want a basis to kind of run from. So...

Q. Did these pen -- penetration tests include the portions of the election system that the Secretary of State is responsible for?

A. Yes, ma'am. The registration side, yes.
Q. Did you personally work with Fortalice on these penetration tests?
A. No. I -- I'm just the client. They're done in a vacuum and then they report back in a draft mode and we talk about them, and then they make a final report.
Q. Did they provide those reports to --
A. To Merritt, yeah. Again --
Q. Did you review --
A. -- that was done because they were the customer.
Q. Correct.
But did you review those reports?
A. I did.
Q. And you said that there were discussions of the reports.
Were you involved in the discussions?
A. I would say most of them, but maybe not all of them.
Q. So to your knowledge, Fortalice conducted and provided a report regarding a penetration test in 2019; is that correct?
A. I would think so, yes.
Q. And in 2020?

A. I'm not sure because of the COVID stuff. I don't know if that happened.

Q. And how about 2021?

A. Again, I don't know.

MS. KAISER: Can you mark Tab 6, please? I'm sorry, Tab 7.

BY MS. KAISER:

Q. We're adding two documents to your folder, Mr. Hamilton. I'd actually like to start with the second one.

A. Okay.

MS. KAISER: 7; is that right?

(Plaintiffs' Exhibit 7 was marked for identification.)

BY MS. KAISER:

Q. Exhibit 7.

A. Okay.

Q. Do you recognize this document?

A. Something I guess from Fortalice. I -- we -- we didn't have Microsoft Teams then. I guess that would be a Fortalice thing.

Q. Yeah, that was one of my questions. It says -- at the top of this page, it says, "This page is automatically updated from the Wiki in Microsoft Teams."

MR. MILLER: Objection. Lack of foundation.

BY MS. KAISER:

Q. Let's see. If you move forward on this document to the February 26, 2021, entry.

A. Okay.

Q. It's on the page ending in -2785.

A. -2785. Okay. I got it.

Q. The last bullet there says, "Weekly update." It says, "vCISO services have been mentioned."

A. Right.

Q. "Kyle and Paul are setting up meeting to discuss with Dave Hamilton to get them caught up on a backlog of security tasks."

Do you --

A. Right.

Q. -- see that?

A. Right.

Q. Do you know what that is referring to?

A. Yeah. I had mentioned to Fortalice that I was planning on leaving the State as soon as I found another position and that they needed to -- you know, as the other partner, if they had the ability to step in.

You know, I wanted to take care of the State. TrustPoint did not have any resources they had left, so there wasn't anybody from our firm. And I checked it out with my boss and he said it would be fine to kick it to them and say, "Listen, you know, we want to take care of our customer and if you're getting ready to leave, then, you know, you need to give it to them."

They subsequently decided that they couldn't fill that seat because of a conflict of interest.

Q. What was the backlog of security tasks that are --

A. I think --

Q. -- mentioned here?

A. I think I pitched to them that there was definitely work to be done, it was a work in progress, and it wasn't going to be -- I think my emphasis there was for -- for them to please be interested, you know.

Because they would want to bill, obviously. They didn't want to just come in and be a -- more of a maintainer than a fixer, right? So my emphasis there was just to kind of get them interested in coming in and stepping in for me.

Q. In your view, why was there a backlog of security tasks?

A. Well, I think it was just, you know, we needed some help. You know, we had some staff turnover and some people leave and I was getting spread pretty thin between there and Imperial and I wasn't there every week, and I just felt like I needed to kind of get people interested in coming to help.

Q. If you move forward in the document to the entry for April 16, 2023 [sic], it's on the page ending in -2784.

A. -2784. Okay. April 16 you said?

Q. 16, yes.

A. Yes, ma'am. Got it.

Q. It says "Project Status," and the second bullet point there says, "Pen test wrapping up."

Do you see that?

A. Okay. Adam Brown. Okay.

Yeah, I worked with --

Q. Does that suggest --

A. -- Adam.

Q. Does that suggest to you that Fortalice did conduct penetration testing in 12 --

A. Sounds like it, yeah.

COURT REPORTER: Thank you.

BY MS. KAISER:

Q. If you go up to the first entry in the document for July 15, 2021.

Do you see that?

The last bullet point there under "Weekly Update," it says, "Red team establishing assumed breach."

Do you see that?

A. What -- I'm sorry. Which page are we on again? I got lost.

Q. Sorry. We're on the first page of the document.

A. Oh, sorry. Okay.

Yep, I got it.

Q. What does, "Red team establishing assumed breach" mean?

A. There's a couple of different ways to approach a client when you're doing red team exercises. And I wanted -- I wanted them to -- or somebody -- probably was me -- wanted them to act like, you know, we had a breach and we needed to also exercise the incident response plan as part of the red team exercise.

Q. What is the incident response plan?

A. It's a set of documentation, policies, procedures that tells people what their roles are. There's certain people that are identified in the organization that kind of -- think of it like everybody heads to the war room and chats about it.

When -- when the security team has an event, that event then -- with further kind of research, if it seems like it is a security issue, then we refer to it as an incident.

It is not the security team's privy to deem something as a breach. We can only show it as a potential breach, and then it's up to management to make that decision whether something is actually a breach. We just -- we just give the facts to leadership and they make the determination whether something's a breach or not.

Only the senior leadership team can implement the incident response plan and kind of move forward with that.

Q. Who is on the -- that management team?

A. Legal -- by name or title? I'm sorry.

Q. Either.

A. Okay. So it would be somebody from legal, somebody from public relations, somebody -- usually two or three people from the senior leadership team,

somebody from operations, service desk. Anybody involved directly in the incident gets drafted into that meeting.

It's just basically to get all the facts out on the table. You whiteboard everything and then you -- there's a playbook that we kind of go by to certify something as real. We score it based on -- it's a judgment, right? We score it based on criticality, and that's how that kind of runs through that program.

Q. And were you part of that management team?

A. I was as the -- as the CISO, yes.

Q. Do you recall what they -- what the results or findings were from Fortalice's 2021 penetration testing?

A. Not -- not by heart. Sorry.

Q. Do you recall anything generally?

A. I think it was just a continuation of the -- you know, the path that they were on. I think they found some new things, I think there were some things from the old report, and then there was things that we fixed. So just part of that journey that I mentioned.

Q. Do you recall whether Fortalice sent a final version of their report from this penetration

know, prioritizing certain remedies and that kind of thing. I just wanted to go back to that for one minute.

A. Sure.

Q. You would agree that the --

A. Sure.

Q. -- Secretary of State is responsible for what's considered critical infrastructure, including the election system, would you not?

A. Yes.

MR. MILLER: Objection. Lack of foundation. Calls for speculation.

BY MS. KAISER:

Q. And do you agree that all reasonable measures should be made to secure such critical systems?

MR. MILLER: Same objection.

THE WITNESS: Reasonable, right, yep, reasonable and appropriate. It's all based on judgment.

BY MS. KAISER:

Q. So you were not suggesting that it's appropriate to leave significant vulnerabilities unmitigated when you're dealing with --

(Cross-talk.)

A. Not at all.
Q. -- critical infrastructure?
MR. MILLER: Objection.
THE WITNESS: Not at all.
BY MS. KAISER:
Q. And you were not suggesting it's appropriate to take no measures to mitigate significant vulnerabilities with critical infrastructure systems?
MR. MILLER: Same objection.
THE WITNESS: Correct, I was not. If we can't fix it one way, there's usually other compensating controls that we can do. So...
BY MS. KAISER:
Q. I have a couple of questions about Georgia's prior election system, by which I mean the DRE voting system.
A. Oh, yeah. I probably won't be much --
Q. Are you aware of any --
A. -- help there, but --
Q. Are you aware of any efforts made by anyone in the Secretary of State's office to determine whether malware was located on any component of the -- of the prior DRE system?
MR. MILLER: I'm going to note an

if you insist, then let the games begin. Fair warning."

Do you see that?

A. Yep.

Q. And it looks like -- it looks like this was sent to soscontact@sos.ga.gov?

A. Right. That's just the -- the basic website. It's like sending a note to the webmaster, right.

Q. Okay. And then this was forwarded on to a group of people, including -- let's see -- including Chris Harvey and Kevin Rayburn.

Do you see that?

A. Yep. James Oliver. Right.

Q. Right.

But you don't recall -- you don't have any recollection of this email or this incident?

A. No, ma'am.

Q. And you don't recall any similar threats during your time at the Secretary of State's office?

A. No, nothing like that. It's been my experience that people who threaten usually don't do it. It's the people that don't say anything that do things like this.

Q. Do you know whether there has ever been a

cybersecurity assessment done of Georgia's voting equipment?

A. I do not. As I understood it, that was the privy of the Dominion folks and that they were independently certified. I don't know much about that process.

Q. So you're not aware of any cyber assess- -- cybersecurity assessment of the voting machines?

A. No, ma'am.

Q. Are you aware of any reports or conclusions regarding any security vulnerabilities with the BMD system?

A. Not -- not specifically, because it kind of fell outside my scope. So...

Q. Are you generally aware of any?

A. No, I -- I can't recall any that -- I mean, there was always the underpinnings of somebody trying to do something, but we live with that every day. So...

Q. So you're not personally aware of any security breaches or vulnerabilities involving the BMD system.

MR. MILLER: Objection. Asked and answered. Lack of foundation.

A. Correct.

Q. Do you know what he meant by that?

A. The actual specific software that goes on there we did not have any experience with, so I think I had asked somebody along the line, I said, "If -- if the vendor should do the install, then let them do the install."

But I would do that with other examples, too. That's probably where that came from.

Q. And when you mean [sic] "the software," you mean the actual EMS software that did --

A. Correct.

Q. -- the ballot design?

A. Yeah. Yeah. So in other words, right, you've got a Windows -- a Windows box that runs Windows and on top of that are individual applications. This would be an individual application on top of that.

(Plaintiffs' Exhibit 13 was marked for identification.)

BY MS. KAISER:

Q. Can you look at the next exhibit, 13?

A. Okay. Hang on. Oh, I don't have that one yet. Hang on.

All right.

Q. And I'll represent to you this was an attachment to the prior email that we were just looking at.

A. Right.

Q. This -- so it says "Site Visit." "Election Office Notes" --

A. Right.

Q. -- "10am 6/15/20 Meeting."

You see that?

A. Right.

Q. And did you recall this meeting -- I mean -- sorry -- do you recall attending that meeting?

A. Vaguely, yeah. I -- I definitely -- this would be like one of my normal hit lists that I list when I go somewhere. Yep.

Q. So do you think that these are notes that you took at that meeting?

A. Yes.

Q. What was the purpose of the meeting?

A. To get a feeling for where he is today and where he wanted to be and how much of a heavy lift it was going to do to -- to get it running.

Q. And when you say "he," you mean --

A. Michael Barnes. I'm sorry. Yeah.

Q. So this was kind of the level set about the project of getting the new servers going for the EMS --

A. Right.

Q. -- software?

A. This was the feedback to the PMO so they could break it into tasks and figure out what other groups needed to help.

And some of the errata I put in here was just typical security guy, head on a swivel, you know, walking around the facility, things I noticed that we could do better. So just a heads up.

And, you know, the idea of giving it back to the PMO would be so he could kind of filter it through the different groups of responsibility. So...

Q. Under "Basic Overview," about -- I think it's about eight bullets down, it says, "No patching of VMware in recent memory, no firmware updating of the hosts, controllers, network gear, etc."

Do you see that?

A. Correct. Yeah.

Q. What did you mean by that?

A. Because it was off-net, they had no way to patch it. They didn't know how, let's put it that

BY MS. KAISER:

Q. So you don't --

MS. KAISER: Sorry, Ms. Barnes. Thank you.

BY MS. KAISER:

Q. So you don't know what it meant that the -- that GEMS was now supported by Dominion?

MR. MILLER: Objection. Lack of foundation.

THE WITNESS: I didn't take that away, I guess, from that meeting. I was just -- I was focused on getting the new stuff loaded.

BY MS. KAISER:

Q. A few bullets down says, "No history of patching anything," and that looks like a frowny face next to it.

A. Yeah. I can do one --

Q. What did you mean --

A. -- right here.

Q. What did you mean by that?

A. It's just a -- it's -- it's basically repeating what he told me. He says there's no -- there's no history of patching anything.

Because there was an assumption that it was off-net, it didn't need to be patched. The

reason people patch is because they're afraid of the Internet. It's not on the Internet; we don't need a patch.

That's not necessarily the way I think, so -- you still gotta be current for the support reasons.

Q. So why did you include a frowny face after that comment?

A. Just -- it's kind of -- for me, when I see a frowny face, it's to kind of remind me that that was a bad thing. Just a note-taking style.

Q. So that was something that you thought needed to be changed?

A. Yes.

Q. Two bullets down from that, it says, "Need to be able to scan every USB attached storage device connected to prior [sic] use. Cannot ensure USB is free from malware, keylogging, etc."

Do you see that?

A. Yes.

Q. What did you mean by that comment?

A. So it was common practice for the -- for the data to be shared with the counties once they drafted or came up with a -- a strawman of what their ballot looks like. They would share that data

via USB. They would, you know, FedEx it to them and then they'd -- they'd mark up changes and then they'd FedEx the USB key back.

Even though Michael had an internal process that when he started the event, he would take a USB drive out of the package and start, he -- he thought that was good enough and -- because he encrypted it and did a lot of other things.

But, you know, I had a different experience in life, so I decided that I thought that he needed to go to a more secure managed solution for USB drives, and I proposed moving to a -- an actual managed USB key program.

And I'm not sure if that ever got funded or not. It was not an insignificant amount of money, but I think they decided that the -- you know, the juice wasn't worth the squeeze, so to speak.

Q. So to -- to your knowledge, at the time you left the Secretary of State's office, that recommendation had not been implemented --

A. No. They had -- they had quotes -- we had quotes and we actually had sample units that Michael Barnes had where he was using it for his work flow to see how it moved.

But I think I left before that decision was made. So...

Q. And why did you make that recommendation?

A. Because he was using commodity-based USB drives.

Q. And why was that not a best practice, in your view?

A. Because they're not made in the U.S. They're -- they could have all kinds of things on them. We don't know.

The only way to really make sure is to, you know, wipe the thing free of -- it has to go through a process of sanitization before you use it.

And, you know, I just -- I really like the idea of a managed USB. The name of it is called DataLocker, and -- and it actually has code on it that you're able to track, much like a LoJack, and it keeps a log of every file ever written and a log -- a file of every -- every time it's read, every time it's loaded, every time anything happens to it, and it uploads it to a cloud-based service so you can see where these drives are; and if someone got ahold of one of these drives and put it in a USB slot that wasn't authorized, that it would wipe the contents securely and -- kind of like bricking a Mac

if you don't -- if you're not the owner kind of deal.

But it was a pretty significant outlay of cash to get that done. And I think he liked the idea. I think -- he wasn't as paranoid as I was. Michael Barnes. Sorry. Didn't mean to say "he."

MS. KAISER: Can you add Exhibit 12, please -- Tab 12?

THE WITNESS: 14.

(Plaintiffs' Exhibit 14 was marked for identification.)

BY MS. KAISER:

Q. If you look at the first email in this chain, it's from Michael Smith at DataLocker.

Do you see that?

A. Yeah, all the way at the bottom? Got it. Okay.

Q. Is this the vendor that you were just discussing?

A. Yes, ma'am.

Q. So it looks like in July of 2020, you reached out to DataLocker and they sent you a response.

A. Correct.

Q. And then your email at the top of

page 1 --

A. Yep.

Q. -- you responded to Michael Smith?

A. Right. Talked about two use cases. Right.

Q. And so this was your explanation of why you were interested in using DataLocker?

A. Correct.

Q. And under -- under item 1 there, you say, "We have a group in the Election Center that uses consumer grade USB flash drives and software encryption to move data regarding ballots and poll information (not votes) to and from the 159 counties in Georgia."

Do you see that?

A. Correct. I do.

Q. Further -- in the next -- top of the next paragraph, you say, "Today these drives are erased and loaded at the EC...."

Do you see that?

A. Right.

Q. Is that the Election Center?

A. It is. Marietta, right.

Q. It says, No. 2, "The environment where these drives are initially populated is currently

air gapped, and my group is reengineering the way that it interacts with the world - maintaining its logical and physical separation."

Do you see that?

A. Correct. Right.

Q. And so the environment that you're talking about there, that's the EMS system that was on the --

A. (Nodded head.)

Q. Yeah. Okay.

A. Correct. Yeah.

Q. -- that was in the Election Center.

So were people in the 159 counties using USB drives to move data in and out of the air-gapped EMS system?

MR. MILLER: Objection. Lack of foundation.

THE WITNESS: Well, yes, but they were provided by Michael's -- Michael Barnes' group. I mean, it's not like the counties are going out and buying their own and using them. It was stuff that was originally provided by Michael. So...

BY MS. KAISER:

Q. But they were using USB drives,

removable --

A. Correct.

Q. -- media.

A. Uh-huh.

Q. Is that consistent --

A. Yeah.

Q. -- with best practices, in your view?

MR. MILLER: Objection. Lack of foundation. Calls for opinion testimony.

THE WITNESS: Yeah, it's -- it -- it's one step above a sneakernet. So, yeah, I mean, I understand why they did it. They didn't want to use email -- I get it -- and they figured that the courier system was more secure and the encryption of the drives and -- you know, he had an erasure kind of process that he went through that we helped kind of tune up a little bit so it does more of a wipe -- a DoD wipe of a drive prior to use.

So it's just -- it's how he had done it for years, and trying to change that was a bit of a challenge.

BY MS. KAISER:

Q. Based on your experience and training, you recommended that the Secretary of State use a vendor

like DataLocker and implement a more secure process; is that right?

A. Correct, yeah. Yeah, if you're going to use a USB drive, it might as well be a managed, FIPS-compliant device, right.

Q. If we can go back for a moment to Exhibit 13.

A. Okay.

Q. I'm just finishing off looking through your notes here.

This is on page 2 --

A. Okay.

Q. -- under "Operational" --

A. Okay.

Q. -- the second bullet. "Data flow into system accomplished by various USB flash drives - not encrypted, not serialized - so no ability to track full lifecycle and pinpoint data loss."

Do you see that?

A. Yeah. They actually are encrypted, but they were not serialized.

Q. And so data was brought into the EMS system through these USB drives; is that correct?

MR. MILLER: Objection. Lack of foundation.

with the IP addresses of -- of people that had accessed the library. And further investigation and once I supplied those to PCC, they were able to validate each one of those IP addresses were their employees. So...

Q. And so the -- the -- what was done to remedy this was just to have PCC pull the --

A. Yeah, to destroy it.

Q. -- pull the --

A. Yeah, to pull it down, right.

Q. Was anything else done to remediate this incident?

A. No. I think -- I -- I know that there were some phone calls that I was not involved in between leadership and SOS and PCC. I'm sure they were not comfortable phone calls, because they were getting -- you know, it was just -- but I wasn't part of the phone call, so that's a Merritt question.

Q. We're going to look at the next exhibit. I believe it's Exhibit 19.

(Plaintiffs' Exhibit 19 was marked for identification.)

THE WITNESS: Okay. I got it. That's a wicked pattern.

BY MS. KAISER:

Q. This is --

A. Okay.

Q. This is a report from Fortalice Solutions. Do you see that?

A. Yes.

Q. Dated July 14, 2020?

A. Right.

Q. If you look at page 2 of the report -- it's the third page of the document, but it says page 2 at the bottom --

A. Okay.

Q. -- under Section 1.1, "Overview," it says, "In June of 2020, Secretary of State Georgia received report of two vulnerabilities in a web application hosted at https://www[.]mvp[.]sos[.]ga[.]gov."

Do you see that?

A. Correct. Yep.

Q. All right. So this is -- the "MVP" is the My Voter Page; is that right?

A. Yes.

Q. And the next sentence says, "Upon attempted remediation, SoSGA requested that Fortalice validate the remediation attempts."

Do you see that?

A. I do.

Q. Do you recall anything about this incident, about --

A. Yeah. Basically --

(Cross-talk.)

A. Basically, we were asking Fortalice to verify what we were being told by PCC as "it's fixed." Because we didn't have the -- the wherewithal to, you know, go through this stem by stem, we got Fortalice to do it as a third -- third party. So...

Q. And what did Fortalice find?

A. They found that actually they had not remediated it sufficiently, and they made a suggestion on how to fix it the right way. And we fed that information back to PCC.

Q. This is in 2020; correct?

A. Probably. Yeah.

Q. Did PCC still have responsibility for the MVP page in 2020?

A. No.

Q. So why did you need to feed the fix back to PCC?

A. Because they still write the code. They

still manage the application, they just don't manage the hardware. So they're still responsible for the code line.

Q. So when you identified a vulnerability on the My Voter Page, you still had to rely on PCC to fix it?

A. Correct.

Q. If you look at page 4 of the Fortalice report --

A. Okay.

Q. -- under "Conclusion," it says, "The remediation attempts that are currently in place partially fix the issues in the original report, but more work needs to be done to secure the website from potential attacks."

Do you see that?

A. Right.

Q. "In addition to the checks performed, Fortalice noticed other areas of potential impact that, while unconfirmed, Fortalice believes could be used to further exploit the site or the servers hosting it. Fortalice recommends having the application thoroughly reviewed for similar issues."

Do you see that?

A. Correct. Right.

Q. Do you know whether that recommendation was accepted, to have the application reviewed for similar issues?

A. I -- I didn't. I didn't have an application-specific review done for them because I -- I think at that point, the decision had been made to jettison PCC.

So I think leadership looked at it as, "We're going away from them, so, you know, we're going to spend the time on the new stuff."

We did feed all this information back to them, that there might be some other areas and, you know, as a partner, we expect them to, you know, find some of their own issues. We don't want to be -- be their QA group. So...

Q. I just want to make sure I understand the timing, because, you know, I -- I've understood you to say that PCC was jettisoned in 2019; is that right?

A. From the operational standpoint, right, the care and feeding of the servers, the patching, that kind of stuff, and the contract of housing the servers and we're paying them to do that service.

But the actual code line, the development and the -- and the -- you know, the changes that

were made to MVP and all those -- OLVR, all those systems, were still under their control because they were the developers.

Q. Right.

And so by 2020, the Secretary of State's office had taken over with respect to the security of these applications; is that right?

A. Well, insofar as we can handle it from the -- from the edge. But as far as internal to the actual application, we still have to rely on PCC to do what they profess they're experts at.

So that's why we run these monthly checks, and what we do with Fortalice with pen tests is to, you know, trust but verify, right? We verify what they told us to be true.

Because the Secretary of State doesn't employ any developers, that's -- that's a bit of a -- a hill to climb. We didn't have anybody in there that wrote code, so we couldn't really challenge them on a code line level. We just identified, "Hey, this doesn't work right; go fix it."

Q. So when --

A. This --

Q. -- Fortalice recommended -- recommended a

thorough application review, is that --

A. Uh-huh.

Q. -- something that the Secretary of State's office could carry out, or would you have to rely on PCC?

A. No, no, no. We would have to actually hire another company to do that as a third party.

So they would take the source code, they would go review the source code and how the program is written, and make recommendations, look at common security vulnerabilities.

There's a term "OWASP." It's for the -- you know, the top 25 things that people do wrong in programs. And they were missing some of the basic stuff, so we started beating up on them about being at least OWASP compliant.

But it would have been a third party. I'm not sure if -- if Fortalice provided that. They -- they may or may not have had that as -- it sounds like it is. It sounds like, "Oh, by the way, you know, we could do this for you," cha-ching, you know, that kind of thing.

Q. But to your knowledge, that kind of thorough review of the application for similar issues to the ones you identified at the time was

never done?

A. Not while I was there. It might have been done after I left, but, again, that's --

Q. You're not aware of that?

A. I'm not aware of it, right.

MS. KAISER: Tab 18, please. I'm adding Exhibit 20.

THE WITNESS: Okay.

(Plaintiffs' Exhibit 20 was marked for identification.)

THE WITNESS: Okay.

BY MS. KAISER:

Q. This is an email from you dated April 29, 2021.

A. Right.

Q. Do you see that?

And it says to Ronnell Spearman, Derek Hawkins, and DeVon King.

A. Right.

Q. And are those -- are those the three security analysts that reported to you --

A. At that --

Q. -- at this time?

A. -- time, right.

COURT REPORTER: One at a time, please.

Q. -- at this risk register?
A. I don't. I don't know who it would have been.
Q. Okay.
A. 8/21/20. Was that around the time that we were doing the litigation? I mean, I don't know if that might have been it. Maybe a lawyer asked for it. I'm not sure.
I was just concerned of it being public, that's all. Just trying to advise.
MS. KAISER: All right. Tab 22, please.
(Plaintiffs' Exhibit 23 was marked for identification.)
THE WITNESS: So that was 21 and 22. This will be 23?
BY MS. KAISER:
Q. Oh, apologies. Yep, this will be 23.
A. Okay. There it is.
Q. Are you familiar with Rule 590-8-3?
A. Uh-huh.
Q. And just generally, what do you -- what do you recall about that rule, what it requires?
A. I think -- I think -- do I put it on here?
Q. Yeah. If you -- on page 3, starting --
A. Yeah.

Q. -- on page 3.
A. The definitions. I just copied the rule into the document. So...
Q. Right. Right.
So Section (b), if you look at the middle of the page, says --
A. Right.
Q. -- "Security of the Voter Registration System is vital to the administration of elections in Georgia. As such, the system shall be maintained in a manner that is consistent with the following security standards."
Do you see that?
A. Yes, ma'am.
Q. And then it lists 27 security standards; right?
A. Right.
Q. And then Section (c), "Assessments," says, "The Secretary of State shall conduct or have conducted regular cybersecurity assessments of the Voter Registration System."
Do you see that?
A. I do.
Q. And then Subsection (d) essentially requires an annual certification of compliance with

the rule; is that right?

A. Correct.

Q. Was it your responsibility to prepare a certification of compliance with Rule 590-8-3?

A. Yes. This is my document, so yes.

Q. And this is the document for 2020; correct?

A. Correct.

Q. Did you prepare a certification like this in any other years?

A. I think 2020 was the -- the only one I did. I think before that, it was somebody else or it got missed. Again, I don't know. I --

Q. On page 6 --

A. Okay.

Q. -- the second paragraph on page 6, it says, "Currently, our agency does NOT meet the requirements of the rule. Out of the 38 requirements we only meet 66%."

Do you see that?

A. Yes.

Q. And so you did an analysis and determined that you only met the -- met the requirements for about two-thirds of the requirements of the rule; is that correct?

A. Correct. Yeah, it says there if we took the Civix-related ones out, we'd be at 81.

Q. And what is Civix?

A. The new name for PCC.

MS. KAISER: Tab 19, please.

(Plaintiffs' Exhibit 24 was marked for identification.)

THE WITNESS: Are we done with that one?

BY MS. KAISER:

Q. Yes. We're adding the next exhibit now, 24.

Do you have that document in front of you?

A. Waiting for it to update.

24. Okay. There it is. Okay.

Q. All right. This is an email chain from December of 2020.

Do you see that?

A. Uh-huh.

Q. And I'm focused on your email on the -- starting on page 1.

A. Okay.

Q. It looks like you were just sharing some thoughts with folks internal to the Secretary of State's office.

Does that look right?

A. It does.

Q. If you look about four paragraphs down, it says, "From a security team perspective, we need more time to focus on the day-to-day operations - all the guys are buried in projects so there is no time to 'watch' or tune things."

Do you see that?

A. Yeah.

Q. What did you mean by this comment?

A. As an example, us having to build the servers over at the Election Center and do a bunch of stuff that are usually infrastructure related. That was supposed to be a pretty quick turnaround and just helping out a brother kind of a thing because they were slammed. It ended up being a very long-term project and Michael Barnes didn't want to let go of us. So it -- it became kind of a resource, you know, drain on all of us.

I think that's probably one of my -- what I was saying here is we -- we really want to hand this back to the infrastructure team. That's why I copied Bill Warwick and Jason and Kevin. So I think this was my, you know, mea culpa of, "Hey, you know, we've got to address a lot of things and there's just not enough hands." So yeah.

Q. What effect did it have on the security team's ability to do its work effectively?

A. Well, I mean, we had to depend on systems, right, instead of people. And luckily we had very good systems, in that we had, you know, Palo Alto, XDR. We had Cortex on the edge. We had multiple layers of security in some cases, where if one thing broke, then we'd still be okay.

But we needed time to continue to tune those as time went on. And the idea there is to reduce the amount of false positives that you get or, even worse, false negatives.

So the idea is it's a -- it's a constant thing, you know, to -- to look at this kind of status of everything on a daily basis and make adjustments.

And I -- I think my note here was just underlying the fact of, "Hey, infrastructure guys, we really need you to do your -- your part in this so we can get back to our real jobs." So...

Q. Are you familiar with a professor at the University of Michigan named Alex Halderman?

A. Yes.

Q. What do you know about Mr. Halderman?

A. He was part of the litigation the last

time around. He had some specific questions that kind of trickled back towards me. It was -- that was the reason I wrote the second document, to clarify some of the things that he assumed.

Q. Did you review any declarations that are -- that were put in by Dr. Halderman?

A. At that time I did, yes.

Q. Have you reviewed any testimony from Dr. Halderman regarding how easily the BMD system can be hacked?

A. No.

MR. MILLER: Objection. Lack of foundation.

BY MS. KAISER:

Q. Were you aware of that testimony?

A. In passing, I think. I -- I -- I don't know if my opinion matters when it comes to that. So...

It's very easy for an academic to control an environment, given enough time and resources and money, to do anything. So that's where the judgment comes in.

So that's what I was trying to get across to the doctor when I responded in that second note, just giving him some clarity about in the

operational world of running a business, we have to do these things and reprioritize.

So that's basically what that was.

Q. Do you understand that Dr. Halderman has analyzed the voting equipment that is used in Georgia today to assess the reliability and security of that equipment?

A. I didn't know that he personally had done it, no. I know --

Q. So you weren't aware that he's issued a detailed report finding that the current system suffers from many significant vulnerabilities?

A. I didn't --

MR. MILLER: Objection. Lack of foundation.

THE WITNESS: Yeah, I -- I didn't. Sorry.

BY MS. KAISER:

Q. You didn't know -- you just didn't know about that report one way or the other?

A. No. I'm not --

MR. MILLER: Objection.

THE WITNESS: -- in the academic world. I don't spend a lot of time reading papers and things like that. So...

BY MS. KAISER:

Q. I'm sorry. It was not a paper, but a report in this case.

A. Yeah, that's fine.

MR. MILLER: Objection. Lack of foundation.

BY MS. KAISER:

Q. So you were not -- not aware of it?

MR. MILLER: Same objection.

COURT REPORTER: The answer again, please?

THE WITNESS: No, I -- I was not aware of it.

COURT REPORTER: Thank you.

BY MS. KAISER:

Q. Do you understand that the current BMD voting system uses QR codes to tally votes?

A. I do --

MR. MILLER: Objection --

THE WITNESS: -- and only because I vote in Georgia. I saw them. So...

COURT REPORTER: The objection again, please?

MR. MILLER: Lack of foundation.

COURT REPORTER: Thank you.

Please -- please let him get in an

objection and her finish the question. Thank you.

THE WITNESS: All right.

BY MS. KAISER:

Q. Are you aware that the current election equipment can be hacked in a way that QR codes can be changed so that they don't reflect what the voter actually intended when they voted on the machine?

MR. MILLER: Objection. Lack of foundation.

THE WITNESS: I did not.

BY MS. KAISER:

Q. Based on your experience and training, if that were the case, would you take measures to eliminate that vulnerability?

MR. MILLER: Objection. Lack of foundation.

THE WITNESS: I don't know if I have enough information, but, yeah, it would definitely go on the list.

BY MS. KAISER:

Q. Would it be a high priority on the list?

MR. MILLER: Same objection.

THE WITNESS: I -- again, it -- it all depends on what else was going on at the time.

So...

BY MS. KAISER:

Q. A vulnerability that would allow a QR code to be changed to change votes, would that be considered high priority?

MR. MILLER: Objection. Lack of foundation. Asked and answered.

THE WITNESS: But the -- the issue is is that -- that system is out of scope for me in my role for Secretary of State. It -- it all belongs to Dominion.

So for them, I would imagine it would cause some heartburn, but not -- I -- out of scope for me.

BY MS. KAISER:

Q. Would it surprise you to learn that the Secretary of State's office has taken no measures to mitigate or eliminate any of the vulnerabilities that Dr. Halderman has found with the existing equipment in Georgia?

MR. MILLER: Objection. Lack of foundation. Form of the compound question. Misstates testimony.

THE WITNESS: Yeah, I -- I -- I don't know what he -- he brought out. I don't know what

on.

BY MS. KAISER:

Q. If you had responsibility for voting equipment and you identified a security vulnerability in that equipment, would you consider that an important thing to -- to fix?

A. Yes.

MR. MILLER: Objection. Lack of foundation. Calls for speculation.

THE WITNESS: Sorry.

BY MS. KAISER:

Q. Your answer was?

A. Yes.

Q. Thank you.

MS. KAISER: All right. Mr. Hamilton, if you'll give us just a minute to confer, I think we're -- we're reaching the end of our questions.

THE WITNESS: Okay.

MS. KAISER: So we'll go off the record for just a minute, please.

VIDEOGRAPHER: The time is 2:15. We're off the record.

(Off the record.)

VIDEOGRAPHER: The time is 2:27. We're

back on the record.

BY MS. KAISER:

Q. Just a few more questions for you, Mr. Hamilton.

Are you aware that Dr. -- Dr. Halderman got access to Fulton County's voting equipment in August of 2020?

A. No, I didn't.

Q. Okay. You were chief information security officer at the time, August 2020; correct?

A. Yes.

Q. All right. And were you aware that Dr. Halderman testified in an evidentiary hearing in September of 2020 about that election -- about vulnerabilities in that equipment?

A. Was that the same one that I did my testifying in or is that a different one?

Q. I'm sorry. Did you ever testify at a hearing?

A. Yes, ma'am. I was -- I had, like, two questions asked of me, but yeah. It was a federal -- I thought it was the Curling case, the initial part of it, with Judge Totenberg. She asked me to clarify a couple of terms. But --

Q. Okay.

A. -- that was when -- that was when we -- we got Zoom bombed that day. Do you recall that?

Q. You know, I wasn't present at the hearing, so I can't recall.

A. Okay.

MS. KAISER: And, Carey, I'm not sure if you recall either if that was the September 2020 hearing.

MR. MILLER: My understanding of the question, I think so, yeah.

MS. KAISER: Okay.

BY MS. KAISER:

Q. Well, so did -- were you present for Dr. Halderman's testimony --

A. No.

Q. -- in a -- in a hearing?

A. No, no, no. I only -- the only people I saw were the ones that were on that day, and he was, I think, on a previous day. That's why I had to respond in writing for his stuff.

Q. And are you aware -- are you aware that he testified that he was able to hack the election equipment from Fulton County?

MR. MILLER: Objection. Lack of foundation. Calls for speculation.

THE WITNESS: Yeah, I -- I didn't realize. No, I didn't hear that.

BY MS. KAISER:

Q. And he was able to do so in just three days?

MR. MILLER: Objection. Lack of foundation. Calls for speculation.

BY MS. KAISER:

Q. You're --

A. And this is the --

Q. -- not aware of that testimony?

A. No. Just as it pertains to that list that I gave.

Q. This is not -- this is not about the list of -- from Fortalice; this is --

A. Okay.

Q. -- this is separate.

A. Yeah. I wasn't present for any of that.

Q. Okay. And you were not made aware of Dr. Halderman's testimony regarding hacking the actual election equipment from Fulton County?

A. No, I was not.

MR. MILLER: Objection. Asked and answered.

THE WITNESS: Sorry.

BY MS. KAISER:

Q. Would you expect to be made aware of that -- of testimony that the election equipment that Georgia had and was using was able to be hacked in three days?

MR. MILLER: Objection. Calls for speculation.

THE WITNESS: Yeah, I would think so.

BY MS. KAISER:

Q. And as -- in your role as chief information security officer for the Secretary of State's office, that's something that you would have liked to know about; is that right?

MR. MILLER: Objection. Calls for speculation.

COURT REPORTER: The answer again, please?

BY MS. KAISER:

Q. But nobody told you about that testimony from Dr. Halderman?

MR. MILLER: Objection. Lack of foundation. Asked and answered.

COURT REPORTER: I didn't hear the previous answer to the question -- the previous question.

THE WITNESS: No. "No" was on both.

Yeah.

COURT REPORTER: Thank you.

MS. KAISER: I just want to make sure, Ms. Barnes -- I'm sorry, I don't have access to the realtime -- which question did you not have an answer to?

COURT REPORTER: One moment, please.

(Whereupon, the record was read by the reporter as follows:

Question, "In your role as chief information security officer for the Secretary of State's office, that's something that you would have liked to know about; is that right?")

THE WITNESS: And I said, yes, that would be nice to know.

BY MS. KAISER:

Q. Do you have any idea why nobody told you about this testimony from Dr. Halderman?

MR. MILLER: Objection. Calls for speculation.

THE WITNESS: I don't.

BY MS. KAISER:

Q. Are you aware of any measures to mitigate the hack that Dr. Halderman executed on the Fulton

County election equipment?

A. No, I --

MR. MILLER: Objection. Lack of foundation. Calls for speculation.

THE WITNESS: No, I -- I would expect that to be a Dominion thing. So...

BY MS. KAISER:

Q. You think -- do you think the Georgia Secretary of State's office would be involved, though?

MR. MILLER: Objection. Calls for speculation.

THE WITNESS: I -- I would think as a customer, yeah.

BY MS. KAISER:

Q. And who within the -- the Georgia Secretary of State's office would have responsibility over that?

A. Over the machines themselves?

Q. Yes, or -- yeah, over identifying or mitigating vulnerabilities with the machines themselves.

MR. MILLER: Objection. Lack of foundation.

THE WITNESS: Yeah, it was my

understanding that all of them are actually owned by the individual counties. So --

But, yeah, I still think the Secretary of State would want to know that information and then do -- you know, get somebody excited about fixing it if that was the case.

BY MS. KAISER:

Q. And the person within the Secretary of State's office under whose purview that would fall, don't you think that would be the chief information security officer?

MR. MILLER: Objection. Calls for speculation. Lack of foundation.

THE WITNESS: I guess if it was in scope, probably, yep.

BY MS. KAISER:

Q. So this shouldn't just be a Dominion thing, as you said earlier; right? That's something that --

A. Well, I mean, it's their -- it's their equipment and it's their code line, so, you know, we can't fix it for them. They would have to do it for us, much like PCC would have to fix their software for us.

Q. But the Secretary of State's office would

have a great interest in making sure that those vulnerabilities were fixed; correct?

A. I would think --

MR. MILLER: Objection --

THE WITNESS: -- so.

MR. MILLER: -- asked and answered. Calls for speculation.

MS. KAISER: Did you get that answer, Ms. Barnes?

COURT REPORTER: I heard, "I would think so."

BY MS. KAISER:

Q. Are you aware, Mr. Hamilton, that Fortalice conducted an assessment of the BMD equipment in 2019?

A. No, actually, not -- you mean the actual polling equipment in the --

Q. (Nodded head.)

A. No, I didn't realize they did that. That must have been on a -- on a separate statement of work.

Q. So you had no involvement with -- with that assessment by Fortalice of the equipment itself?

A. No. And it might be just because it was

excluded from my statement of work from TrustPoint. You know, it was specifically excluded that the actual voting tabulating, Dominion or whatever, was excluded from my responsibilities.

MS. KAISER: All right. Just one -- one more minute, Mr. Hamilton. Thank you.

THE WITNESS: Okie doke.

VIDEOGRAPHER: Would you like to go off the record, Counsel, or stay on?

MS. KAISER: [Inaudible], please.

VIDEOGRAPHER: I'm sorry. You broke up.

MS. KAISER: I said go off the record, please.

VIDEOGRAPHER: The time is 2:35. We are off the record.

(Off the record.)

VIDEOGRAPHER: The time is 2:38. We're back on the record.

BY MS. KAISER:

Q. Mr. Hamilton, just -- I just want to make sure the record is clear.

You're not aware of any request by anyone from the Secretary of State's office to Dominion to fix any of the vulnerabilities that Dr. Halderman identified with the Fulton County voting equipment;

is that correct?

A. That is --

MR. MILLER: Objection --

THE WITNESS: -- correct.

MR. MILLER: -- lack of foundation.

THE WITNESS: I -- I don't recall any conversation specific to Fulton County except for that notebook we talked about.

BY MS. KAISER:

Q. That was a laptop.

A. Laptop, yeah, notebook. Sorry.

Q. Right.

So with respect to the Fulton County voting equipment that Dr. Halderman tested and was able to hack, you don't recall any instruction to Dominion to fix anything related to that?

A. No.

MR. MILLER: Objection. Lack of foundation. Asked and answered.

THE WITNESS: No.

MS. KAISER: All right. No further questions from me, Mr. Hamilton. Thank you very much for your time today.

THE WITNESS: Thank you.

MR. MILLER: Dave, I'm going to have a

I've got it correlated now.

Q. Okay. And have you ever done any work on BMDs?

A. No. I've seen them, you know, as a voter, but...

Q. Right.

And so as the voter, you have some familiarity with what the BMD is; right?

A. Correct.

Q. And that would be the touchscreen computer; right?

A. Right, iPad or Android, depending on where you go, I guess.

Q. And when you vote on those devices, you understand there's a printer connected to that device; right?

A. Right, HP printer. I've seen them.

Q. And then you understand that that printer prints a ballot to the voter; right?

A. Correct.

Q. And then as a voter, you then took that ballot to a scanner; right?

A. Correct.

Q. And so just that I'm -- so that I'm clear, you've -- in your scope of work with the Secretary,

you never worked on the ballot-marking devices themselves?

A. No, sir, not in any --

Q. Never worked on the printer?

A. Nope.

Q. Never worked on the scanner into which the ballots were fed?

A. No, sir.

Q. Okay. And was that type of work beyond your work scope?

A. It was.

Q. So Ms. Kaiser asked you a couple of questions concerning Dr. Halderman.

Do you recall that?

A. Yes.

Q. Are you aware that the report he worked on concerned hacking of that same voting equipment?

A. I -- I didn't correlate the two, no.

Q. Okay. Knowing that, that would then be outside of your work scope; right?

A. Yes.

Q. You talked earlier with Ms. Kaiser about the EMS system.

Do you recall that?

A. Uh-huh.

Q. And I'm going to ask you for an audible answer there.

A. Yes. I'm sorry.

Q. And do you recall discussing with her ballot building or ballot configuration? Do you recall that?

A. Yes, sir.

Q. And am I correct that you've never done any of that ballot building yourself?

A. No, not at any time.

Q. Okay. And so when you talked today about your understanding of that process, was that based on an understanding gleaned from others?

A. Yes.

Q. Ms. Kaiser asked you earlier about a situation in Cobb County.

Do you recall what I'm talking about?

A. Yes. About the vulnerability, yes.

Q. Yeah. Okay.

And do you understand what that vulnerability made visible?

A. Yes.

Q. And what was that?

A. Another person's voter registration information.

C E R T I F I C A T E

STATE OF GEORGIA:

COUNTY OF FULTON:

I hereby certify that the foregoing transcript was taken down, as stated in the caption, and the questions and answers thereto were reduced to typewriting under my direction; that the foregoing pages represent a true, complete, and correct transcript of the evidence given upon said hearing, and I further certify that I am not of kin or counsel to the parties in the case; am not in the regular employ of counsel for any of said parties; nor am I in anywise interested in the result of said case.

LEE ANN BARNES, CCR B-1852, RPR, CRR, CRC